

March 7, 2011

Ryan W. King  
202-457-5312  
[rking@pattonboggs.com](mailto:rking@pattonboggs.com)

**Via ECFS**

Ms. Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Suite TW-A325  
Washington, D.C. 20554

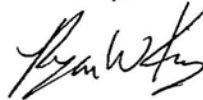
**RE: Annual 47 CFR 64.2009(e) CPNI Certification for 2011  
EB Docket No. 06-36**

Dear Secretary Dortch:

Pursuant to Section 64.2009(e), please find enclosed DigitalBridge Communications Corp.'s (Filer ID # 827208) annual CPNI compliance certificate and accompanying statement of operating procedures for 2011 covering the prior calendar year 2010.

If you have any questions, please contact me at 202-457-5312.

Sincerely,



Ryan W. King  
Associate

cc: Best Copy and Printing, Inc.

# **DigitalBridge Communications Corp.**

## **Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

### **EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2011 covering the prior calendar year 2010

1. Date filed: March 7, 2011
2. Name of company(s) covered by this certification: DigitalBridge Communications Corp.
3. Form 499 Filer ID: 827208
4. Name of signatory: William F. Wallace
5. Title of signatory: Executive Vice President Policy & External Affairs
6. Certification:

I, William F. Wallace, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed William F. Wallace

**Attachments:** Accompanying Statement explaining CPNI procedures

### **Accompanying CPNI Compliance Statement**

Pursuant to Section 64.2009(e) of the Federal Communications Commission's ("FCC") rules, this statement explains how DigitalBridge Communications Corp.'s ("DBC") operating procedures ensure compliance with Part 64, Subpart U of the FCC's rules. DBC prohibits the use of its VoIP customers' CPNI for marketing purposes by itself and between its affiliates.

DBC's CPNI Policies and Procedures Manual includes an explanation of what CPNI is and when it may be used without customer approval. Employees with access to DBC's VoIP customers' CPNI have been trained as to when they are and are not authorized to use CPNI. DBC's CPNI Policy Manual describes the disciplinary process related to noncompliance with CPNI obligations, and sets forth the penalties for non-compliance, which can include termination of employment. DBC has established a supervisory review process regarding DBC compliance with the FCC's CPNI rules. DBC requires affirmative written/electronic subscriber approval for the release of CPNI to DBC's joint venture partners, independent contractors, or third parties.

William F. Wallace, a corporate officer, has been named as the CPNI Compliance Officer and is held responsible for annually certifying that DBC is in compliance with the FCC's CPNI rules and submitting the certification and an accompanying statement explaining how DBC complies with the FCC's CPNI rules by March 1.

Prior to any solicitation for customer approval, DBC provides notification to the customer of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. DBC maintains written record of any notification for at least one year. DBC understands that individual notice to customers must be provided when soliciting approval to use, disclose or permit access to a customer's CPNI.

DBC takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. DBC authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

DBC only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, DBC only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without DBC's assistance, then DBC is permitted to discuss the call detail information provided by the customer.

DBC has established a system of passwords and password protection. For all new VoIP customers, DBC requests that the customer establish a password at the time of service initiation. DBC initiated VoIP service on July 23, 2008. DBC did not have existing VoIP customers when the FCC's new CPNI rules went into effect. For VoIP customers that elected not to establish a password at initiation to now establish a password, DBC must first authenticate the customer without the use of readily available biographical information or account information. DBC authenticates a customer using non-public information such as calling the customer at the telephone number of record or using a Personal Identification Number (PIN) method to authenticate a customer. For accounts that are password protected, DBC cannot obtain the password by asking for readily available

biographical information or account information to prompt the customer for his password. A customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. If a password is forgotten or lost, DBC uses a back-up customer authentication method that is not based on readily available biographical information or account information. If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking DBC to send the call detail information to an address of record or by DBC calling the telephone number of record.

DBC password-protects online access to all CPNI, call detail and non-call detail.

DBC may provide its VoIP customers' with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

DBC notifies a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record.

In the event of a CPNI breach, DBC delays customer notification of breaches until law enforcement has been notified of a CPNI breach. DBC will notify law enforcement of a breach of its customers' CPNI within seven business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct DBC not to disclose the breach for an initial 30-day period. The law enforcement agency must provide in writing to DBC its initial direction and any subsequent direction. DBC may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if DBC believes there is an extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm.

DBC maintains a record of any discovered breaches and notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two year.